US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT Federal Information Notice FIN-06-220-01A
August 8, 2006, Updated August 10, 2006

Vulnerability in Microsoft Windows Operating System (U//FOUO)

Overview (U//FOUO)

A stack-based buffer overflow exists in Microsoft's Remote Procedure Call implementation. This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary code with system privileges.

Description (U//FOUO)

There is a stack-based buffer overflow in Microsoft's Remote Procedure Call (MSRPC) implementation. MSRPC provides a mechanism which allows a program to execute a procedure on a remote system in a way that is transparent to the calling program. Additionally, Windows services that use MSRPC may use Server Message Block (SMB) named pipes as the transport service for MSRPC calls.

A remote attacker could send a specially crafted packet to a vulnerable Windows system, which could trigger the overflow. As this vulnerability involves a Windows networking API, the potential for exploitation is high and the subsequent impact could be severe to an agency's security posture.

An attacker could use this vulnerability to execute arbitrary code on a vulnerable system. This would allow the attacker to perform a variety of nefarious actions, including program installation, data corruption, and the creation of accounts with system level privileges.

US-CERT is aware of working exploit code targeting this vulnerability; however, the specific exploit code has only targeted the Windows 2000 operating systems and only one incident report has been attributed to it to date.

Affected Systems

Microsoft Windows 2000 Service Pack 4

Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

Microsoft Windows XP Professional x64 Edition

Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

Microsoft Windows Server 2003 x64 Edition

Associated Vulnerability

US-CERT VU#650769

For More Information

Contact: US-CERT Operations

Email: soc@us-cert.gov
Voice: 1-888-282-0870
Web: http:www.us-cert.gov

Recommendations (U//FOUO)

US-CERT recommends that all organizations immediately apply the recent patch (MS06-040) released by Microsoft on 8 August, 2006.

If an agency cannot patch immediately, US-CERT urges the use of best practices to ensure a more defensible network posture. Recommended actions include:

1. **Block TCP ports 139 and 445 at the firewall.** This port is used to initiate a connection with the affected protocol. Blocking them at the firewall, both inbound and outbound, will help prevent systems that are behind that firewall from attempts to exploit this vulnerability. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports, visit this Microsoft site: http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/documentation/windows/2000/server/reskit/en-us/cnet/cnfc_por_gdqc.asp.

2. **Enable advanced TCP/IP filtering on systems.** You can enable advanced TCP/IP filtering to block all unsolicited inbound traffic. For more information about how to configure TCP/IP filtering, see http://support.microsoft.com/kb/309798.

3. **Block the affected ports by using IPsec on the affected systems.** Use Internet Protocol security (IPsec) to help protect network communications. Detailed information about IPsec and about how to apply filters is available in http://support.microsoft.com/kb/313190 and http://support.microsoft.com/kb/813878.

4. **Disable anonymous SMB access.** See http://support.microsoft.com/kb/q246261 for information about configuring anonymous access in Windows 2000. Note this will not prevent authenticated users from exploiting this vulnerability, and may have adverse affects in mixed-mode domains.

5. All anti-virus and anti-spyware applications should be updated with the latest definitions.

6. Systems should be monitored or inspected for suspicious accounts not authorized by organizational policy.

7. User education & awareness. Strange and/or unsolicited e-mails should not be opened pending review by security personnel.

8. Intrusion detection systems should be constantly monitored for “out of scope” activity, that is, network behavior not falling within the realm of normal activity.

9. Other workarounds are available in Microsoft Security Bulletin MS06-040.

To date, US-CERT is aware of exploits targeting the Windows 2000 platform only, and as such, has developed Snort signatures to aid in detecting attempted attacks.

```
alert tcp any -> any $RPC_PORTS (msg:"US-CERT Wk2 Overflow Indicator"; content:"| 90 90 EB 04 2B 38 03
78 |";  classtype:malicious-activity; sid:1000003; rev:1;)
```

All activity against these signatures should be treated as a potential Category 1 (one) intrusion and reported to the US-CERT Operations team.

August 10, 2006 Update (U//FOUO)

Exploits targeting the vulnerability described in this notice have been posted to security sites. The Metasploit Project has posted a new exploit module for their exploit framework. The Metasploit Project distributes a tool that provides a graphical user interface (GUI) framework. This GUI framework is used to automate the process of exploiting vulnerable systems.

Additionally, eEye has released a free vulnerability scanner that searches for the MS06-040 vulnerability. US-CERT has tested the functionality of the eEye NetApi32 scanner and determined that it does detect vulnerable systems on a network. US-CERT is currently testing the scanner to see if it adversely affects the system it is installed on or the system it scans.

US-CERT also observed a 50% increase in traffic inbound to port 139 between 0200 and 1100 UTC today (2200 and 0700 EDT). This traffic may be related to the MS06-040 vulnerability and subsequent public exploit code that has been released.

Report to US-CERT (U//FOUO)

Please report any suspected compromised to US-CERT immediately.

US-CERT Contact Information

For reporting incidents:

Email: soc@us-cert.gov
Voice: 1-888-282-0870
Web: http:www.us-cert.gov

WARNING: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C.552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need to know” without prior approval of the US-CERT Operations Center at 1-888-282-0870. No portion of this report should be furnished to the media, either in written or verbal form.